IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

ALFONSO CIOFFI, et al.	§	
	§	
v.	§	CASE NO. 2:13-CV-103-JRG-RSP
	§	
GOOGLE INC.	§	
	§	

CLAIM CONSTRUCTION MEMORANDUM AND ORDER

On August 14, 2014, the Court held a hearing to determine the proper construction of the disputed claim terms in United States Patents No. RE43,103, RE43,500, RE43,528, and RE43,529. After considering the arguments made by the parties at the hearing and in the parties' claim construction briefing (Dkt. Nos. 56, 66, and 67),[1] the Court issues this Claim Construction Memorandum and Order.

[1] Citations to documents (such as the parties' briefs and exhibits) in this Claim Construction Memorandum and Order refer to the page numbers of the original documents rather than the page numbers assigned by the Court's electronic docket unless otherwise indicated.

Table of Contents

BACKGROUND

Plaintiffs bring suit alleging infringement of United States Patents No. RE43,103 ("the '103 Patent"), RE43,500 ("the '500 Patent"), RE43,528 ("the '528 Patent"), and RE43,529 ("the '529 Patent") (collectively, the "patents-in-suit").

All four patents-in-suit are reissues of United States Patent No. 7,484,247 ("the '247 Patent"), which issued on January 27, 2009, from an application filed August 7, 2004. All five patents are titled "System and Method for Protecting a Computer System from Malicious Software."

The '103 Patent issued on January 10, 2012, from an application filed August 10, 2010. The '500 Patent issued on July 3, 2012, from an application filed March 9, 2010. The '528 Patent and the '529 Patent both issued on July 17, 2012, the first from an application filed March 9, 2010, and the second from an application filed November 7, 2010.

The Abstracts of the four patents-in-suit and the '247 Patent are the same and state:

> In a computer system, a first electronic data processor is communicatively coupled to a first memory space and a second memory space. A second electronic data processor is communicatively coupled [to] the second memory space and to a network interface device. The second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device. A video processor is adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display terminal for displaying the combined video data in a windowed format. The computer system is configured such that a malware program downloaded from the network and executing on the second electronic data processor is incapable of initiating access to the first memory space.

The four patents-in-suit, as well as the '247 Patent, share a substantially identical specification.[2] The parties' briefing cites the specification of the '247 Patent. This Claim

[2] The '529 Patent includes a "Term Description" section that does not appear in the other patents.

Construction Memorandum and Order therefore cites the specification of only the ‘247 Patent unless otherwise indicated.

LEGAL PRINCIPLES

“It is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the invention to which the patentee is entitled the right to exclude.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To determine the meaning of the claims, courts start by considering the intrinsic evidence. *See id.* at 1313; *see also C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc’ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). The intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312-13; *accord Alloc, Inc. v. Int’l Trade Comm’n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term’s context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can aid in determining the claim’s meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term’s meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314-15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* at 1315 (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Phillips*, 415 F.3d at 1315 (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *accord Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* The specification may also resolve the meaning of ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex*, 299 F.3d at 1325. But, "[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *accord Phillips*, 415 F.3d at 1323.

The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent."). "[T]he prosecution history (or file wrapper) limits the interpretation of claims so as to exclude any interpretation that may have been disclaimed or disavowed during prosecution in order to obtain claim allowance." *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985).

Although extrinsic evidence can be useful, it is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317 (citations and internal quotation marks omitted). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition are entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

THE PARTIES' STIPULATED TERMS

The parties have reached agreements as to several terms, as stated in their June 2, 2014 Patent Local Rule 4-3 Joint Claim Construction and Prehearing Statement (Dkt. No. 52 at 1-2) and their August 11, 2014 Joint Claim Construction Chart (Dkt. No. 68, Ex. A at 5). The parties' agreements are set forth in Appendix A to this Claim Construction Memorandum and Order.

CONSTRUCTION OF DISPUTED TERMS

As submitted by the parties, most of the disputed terms appear in all of the asserted claims of one or more of the patents-in-suit, as set forth as to each disputed term, below. In the parties' Joint Claim Construction and Prehearing Statement, Defendant identified the asserted claims as follows:

> The asserted claims of the ‘500 Patent are Claims 21, 23, 25, 29, 30, 31, 32, 37, 38, 39, 41, 42, 43, 52, 66, 67 and 70.
>
> The asserted claims of the ‘528 Patent are Claims 1, 2, 5, 21, 23, 25, 30, 44, 46, 52, 53, 55, 57, 58, 64, 65, 66, 67 and 70.
>
> The asserted claims of the ‘529 Patent are Claims 21, 23, 28, 30, 36, 38, 45, [and] 49.
>
> The asserted claim of the ‘103 Patent is Claim 21.

(Dkt. No. 52, Ex. B at 1 nn.2-5.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with preliminary constructions of the disputed terms with the aim of focusing the parties’ arguments and facilitating discussion. Those preliminary constructions are set forth within the discussion of each term, below.

A. “web browser process”

Plaintiffs’ Proposed Construction	**Defendant’s Proposed Construction**
No Construction: Plain and ordinary meaning	“process that performs the retrieval of web pages”[3]

(Dkt. No. 56 at 7; Dkt. No. 66 at 18.) Plaintiffs submit that this disputed term appears in all asserted claims of the ‘500, ‘528, and ‘529 Patents. (Dkt. No. 56 at 7 n.13.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary construction: “process that can access data on websites.”

[3] Defendant submits in its briefing: “To address Plaintiffs’ stated concern about unduly limiting the functions of the web browser process, [Defendant] is amenable to an alternate construction that requires the web browser process to be capable of ‘at least’ performing the retrieval of web pages or a construction that merely acknowledges that the web browser process claimed ‘cannot be a secure renderer.’” (Dkt. No. 66 at 20 n.14.)

(1) The Parties' Positions

Plaintiffs argue that "Defendant's proposed construction seeks to import a discussion of 'retrieval of web pages' from the prosecution history into the claim meaning, and in doing so, completely ignores the fact that the claims themselves describe the web browser process." (Dkt. No. 56 at 8.) Plaintiffs further submit:

> The plain meaning of web browser process would certainly include, among other attributes, the capabilities of (1) accessing data of at least one website via the network, and (2) generating video data from the at least one website accessed via the network. While the inventors have expressly identified these characteristics of the claimed web browser process depending on whether it is the first web browser process or the second web browser process, they in no way altered the plain and ordinary meaning of this commonly understood term.

(*Id.*)

As to the prosecution history regarding the "Narin" reference (United States Patent Application Publication No. 2002/0002673), cited by Defendant, Plaintiffs argue that the patentees "argued that Narin consistently teaches away from the first logical process ever being a web browser process," and "[n]owhere did they say their invention is different because the first logical process must retrieve web pages." (*Id.* at 9.) Plaintiffs further submit that "they were distinguishing Narin on the basis that their first browser process could access Internet sites and/or data (not specifically retrieval of web pages)." (*Id.* at 10.) Plaintiffs conclude: "To be sure, a web browser process may retrieve web pages but the requirement that it must does not flow from the intrinsic evidence." (*Id.*)

Defendant responds that "[d]uring reissue prosecution, the Applicants distinguished prior art reference Narin by explaining that the Applicants' 'browser process' was different than

Narin's rendering process because it performed the retrieval of web pages." (Dkt. No. 66 at 18.)[4] More specifically, Defendant argues, "the prosecution history makes clear that the term 'web browser process' was intended to be narrower than the 'browser process' language previously used in the claims." (*Id.* at 19.) Defendant concludes that "a construction that gives effect to the addition of the word 'web' must be adopted to make clear that both the first and second 'web browser' processes exclude a renderer, like the one in Narin, that does not perform the retrieval of web pages." (*Id.* at 20.) Finally, Defendant submits that its proposed construction does not limit "the web browser process to only performing the retrieval of web pages" but rather "permits the process to perform any of the other web browsing functions that Plaintiffs recite." (*Id.*)

Plaintiffs reply that the prosecution history relied upon by Defendant "is nowhere close to the inventors stating their browser processes are distinct from Narin because they 'retr[ie]ve web pages' as Defendant would have the Court believe." (Dkt. No. 67 at 1-2.) Plaintiffs also argue: "The inventors responded [to the examiner's rejection] by adding 'web' in[]front of 'browser process' and making the first web browser process 'capable of accessing data of a website via the network.' Defendant's focus on the addition of the term 'web' does not tell even half the story as to why the rejections were made and what the inventors did in response." (*Id.* at 2.) Further, Plaintiffs note, Defendant's proposed construction "renders the language 'capable of accessing

[4] The "secure rendering process" in Narin is, for example, an application for playing audio or video content that is protected by Digital Rights Management (DRM). *See* Narin at ¶ 46. "Such a system must protect itself and the content from attacks—i.e., the application must resist attempts by a hacker to 'steal' decrypted content or a decryption key. Since the decrypted content and/or the key may be stored in memory (e.g., in the address space of the process that runs the application), unknown or non-secure executable objects cannot be granted access to that address space, and thus cannot run in the same process as the secure rendering application." *Id.*

data of the at least one website via the network' irrelevant because that capability is already implied by being able to carry out the narrower function of retrieving web pages." (*Id.* at 2 n.3.)

(2) Analysis

The specification uses the terms "web browser" and "website" but does not define those terms:

> [T]here may be a variety of files that a user may wish to have automatically cleaned or deleted upon closing a protected process session. For example, temporary internet files, cookies, browser plug-ins, etc., may be deleted or scanned for malware automatically. A user may also wish to have *websites* that contributed to a malware infection noted, and may wish to place the offending *websites* in a block list, such that the offending *websites* cannot be accessed in the future without the user specifically authorizing access. As part of the malware scan, the malware scanner may automatically log the offending *website(s)*, and block future access.
>
> * * *
>
> Referring again to FIG. 9, the functions carried out by processors 920 and 940 may comprise separate, secure logical processes executing on the same physical processor. For example, a first logical process may comprise executing instructions necessary to carry out the functions of an operating system, or the first logical process may comprise executing instructions necessary to carry out the functions of a first computer program, including but not limited to a word processor. A second logical process may comprise executing instructions necessary to carry out the functions of a *web browser* program, or may comprise executing instructions necessary to carry out the functions of an instant messenger program, for example.

'247 Patent at 13:53-64 & 16:22-34 (emphasis added).

During prosecution of the reissue application that led to the '528 Patent, the examiner cited the "Narin" reference (United States Patent Application Publication No. 2002/0002673) as a basis for rejecting various claims. (*See* Dkt. No. 57-3, Ex. C, 4/29/2011 Office Action at ¶¶ 10-59.) As explained by the patentees, Narin discloses running a "closed or protected application" that controls a separate auxiliary process that runs an "open or untrusted application." (Dkt. No. 58-1, Ex. D, 8/29/2011 Amendment Under 37 CFR §1.111 at 21.) In particular, Narin discloses:

> FIG. 3 shows a secure application which uses a non-secure software object to perform an action or provide a service. Secure application 312 runs inside process 310. Application 312 is "secure" in the sense that it includes some type of defense against observation or modification. For example, secure application 312 may be an application that renders encrypted content, and which prevents or deters a user from learning the decryption key used to decrypt the content, or from copying the decrypted content itself. Typically, secure application 312 is relied upon by some system (e.g., a digital rights management system, or the participants therein) to behave in a predictable way (e.g., the distributors of content in a digital rights management system may rely on secure application 312 to render content only when permitted by the terms of a license). Secure application 312 may, optionally, host a software object 314.

Narin at ¶ 35.

The patentees argued:

> . . . Narin teaches away from the closed process being a browser process.
>
> * * *
>
> Narin describes a web browser as being an example of . . . a non-secure software object, meaning that a web browsing program cannot be part of the secure application.
>
> * * *
>
> Narin . . . draw[s] the clear distinction between a web browser and a secure application, again, clearly teaching away from the secure application ever being a web browser process.
>
> * * *
>
> Narin makes the clearest distinction below between the browser and the secure application, referring to the web browsing function as being a separate program running in a separate process. Narin here is clearly teaching away from the secure application and the non-secure application both comprising browser processes.

(Dkt. No. 58-1, Ex. D, 8/29/2011 Amendment Under 37 CFR §1.111 at 21, 22, 23 & 24.) The patentees also quoted various passages from Narin, including the following:

> If the user clicks on any of the links, the browsing program will retrieve the web page associated with that link and display it to the user. It should be observed that it is the browsing program, and not the secure rendering application, that performs the retrieval of web pages.

(*Id.* at 24 (quoting Narin at ¶ 49); *see also* Dkt. No. 66, Ex. 14, ’500 Patent File History, 10/13/2011 Amendment Under 37 CFR §1.111 at 17 (same).)

After the patentees made these amendments and arguments, the examiner again rejected claims based on Narin, noting that “the features upon which applicant relies, such as the first browser process accessing Internet sites and/or data, are not recited in the rejected claims.” (*See* Dkt. No. 59-1, Ex. E, 11/14/2011 Office Action at ¶ 8; *see also* Dkt. No. 66, Ex. 17, ‘500 Patent File History, 11/17/2011 Office Action at ¶ 5 (“Throughout his arguments, the Applicant makes reference that the first browser process is a web process. It is noted that the features upon which applicant relies, that the claimed browsers are actually *web* browsers, are not recited in the rejected claims.”); *id.* at ¶ 7 (“[T]he secure rendering application of the prior art does teach the first browser process in a first logical process when that limitation is interpreted in light of the specification to include web browsers, video games, and word processing applications.”).)

The patentees responded by amending the claims so as to recite a “web” browser rather than simply a browser, and the patentees further added that the first web browser process is “capable of accessing data of a website via the network.” For example, the patentees amended Claim 1 of the ‘528 Patent as follows (additions underlined, as in original):

> 1. (Currently Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising:
>
> executing a first web browser process, capable of accessing data of a website via the network, in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space;

> executing a second web browser process in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space; and
>
> displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display;
>
> wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

(*See, e.g.*, Dkt. No. 60-1, Ex. F, 1/24/2012 Amendment Accompanying RCE at 28.)

Thus, the patentees relied on claiming a "web" browser process, and that reliance should be given effect by requiring that a "web browser process" is capable of accessing data on websites. *See Typhoon Touch Techs., Inc. v. Dell, Inc.*, 659 F.3d 1376, 1381 (Fed. Cir. 2011) ("The patentee is bound by representations made and actions that were taken in order to obtain the patent."); *see also Southwall Techs. Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1576 (Fed. Cir. 1995) ("Claims may not be construed one way in order to obtain their allowance and in a different way against accused infringers."); *Jansen v. Rexall Sundown, Inc.*, 342 F.3d 1329, 1333 (Fed. Cir. 2003) (finding that where "phrase[s] were added to gain allowance of the claims after . . . repeatedly unsuccessful attempts to gain allowance of claims without those phrases[,] [w]e must . . . give them weight, for the patentability of the claims hinged upon their presence in the claim language"); *Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1374 (Fed. Cir. 2007) ("An applicant's invocation of multiple grounds for distinguishing a prior art reference does not immunize each of them from being used to construe the claim language. Rather, as we have made clear, an applicant's argument that a prior art reference is distinguishable on a particular ground can serve as a disclaimer of claim scope even if the applicant distinguishes the reference on other grounds as well.").

Defendant has failed, however, to establish that the constituent term “web” necessarily refers to “web pages.” The Court rejects Defendant’s proposal in that regard.

At the August 14, 2014 hearing, Defendant stated that it could agree to the Court’s preliminary construction with an understanding that the construction refers to “direct” access. Plaintiffs responded that they could agree to the Court’s preliminary construction with an understanding that the construction does *not* require “direct” access. The parties’ reactions to the Court’s preliminary construction thus revealed a dispute as to whether a “web browser process” must be able to access websites “directly.”

On balance, introducing the word “direct” would tend to confuse rather than clarify the scope of the claims. *See U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997) (“Claim construction is a matter of resolution of disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement.”). Also, Plaintiffs have noted that Claim 21 of the ‘528 Patent, for example, recites, in relevant part (emphasis added): “wherein the first web browser process is capable of opening the second web browser process and is further capable of *passing data to the second web browser process*.”

To be clear, “can” in the Court’s construction does not mean “must” and instead refers to a capability. For this capability to be meaningful and consistent with the prosecution history, however, a “web browser process” must be capable of accessing a website without using another web browser process. In other words, although the Court’s construction does not *preclude* a web browser process from accessing websites by using another web browser process, a web browser process’s capability of accessing websites must not *require* using another web browser process.

The Court thus hereby construes **"web browser process"** to mean **"process that can access data on websites."**

B. "wherein the second web browser process is capable of accessing data contained in the second memory space"[5]

Plaintiffs' Proposed Construction	Defendant's Proposed Construction
No Construction: Plain and ordinary meaning	"wherein the second web browser process is only capable of accessing data in the second memory space"

(Dkt. No. 56 at 10; Dkt. No. 66 at 23.) Plaintiffs submit that this disputed term appears in all asserted claims of the patents-in-suit. (Dkt. No. 56 at 10 n.20.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary construction: "Plain meaning [Expressly reject Defendant's proposal that the second web browser can access only the second memory space]."

(1) <u>The Parties' Positions</u>

Plaintiffs submit that "[a]ll the asserted independent claims clearly state that the second web browser process 'is capable of accessing data contained in the second memory space' but say nothing about the second web browser process being limited to 'only' accessing data contained in the second memory space." (Dkt. No. 56 at 10-11.) Plaintiffs further argue that "the specification flatly contradicts Defendant's proposal and teaches that the second web

[5] In their Joint Claim Construction and Prehearing Statement, as well as in their Joint Claim Construction Chart, the parties submit this disputed term together with the following disputed terms: "wherein the second web browser process is configured to access data contained in the second memory space"; "wherein the second logical process is capable of accessing data contained in the second memory space"; "the second logical process being configured to access data contained in the second memory space"; "at least one second protected web browser process is configured to access data contained in the second protected memory space"; and "at least one secure browser process configured to: . . . access data contained in the second memory space." (Dkt. No. 52, Ex. A at 3-4; Dkt. No. 68, Ex. A at 4.)

browser process could access the first memory space, for example, provided the user gives permission." (*Id.* at 11-12.)

Defendant responds that "[t]o accept Plaintiffs' proposed construction would be to contradict the security principles taught by the invention and allow the second process to corrupt trusted content on the first memory space." (Dkt. No. 66 at 24.) Instead, Defendant argues, "[t]o protect the files on the first memory space, the second web browser process can *only* have access to the second memory space." (*Id.*) If the claims are construed otherwise, Defendant urges, "the reissued claims are indefinite because they contradict the core security teachings of the invention." (*Id.* at 26.) Defendant further submits that "the intrinsic evidence states that the computer system is only configured in an 'unprotected mode' when there are no network processes active," whereas all of the claims at issue require active network processes. (*Id.* at 25.)

Plaintiffs reply that "every claim requires that the second web browser process running the malware not be automatically capable of accessing the first memory space." (Dkt. No. 67 at 4.)

At the August 14, 2014 hearing, Plaintiffs argued that if the Court adopts its preliminary constructions as to the "first memory space" and "second memory space" terms (discussed below), then Defendant's proposal is unnecessary. Defendant nonetheless expressed concern that if the Court rejects Defendant's proposed construction as to the present disputed term, Plaintiffs might identify a memory space that is accessible by both the first and second web browser processes.

(2) Analysis

Claim 21 of the '500 Patent recites (emphasis added):

> 21. A portable computing and communication device capable of executing instructions using a common operating system, comprising:

> a network interface device configured to exchange data across a network of one or more computers using a wireless connection;
>
> an intelligent cellular telephone capability with a secure web browser including a first web browser process and a second web browser process;
>
> at least a first memory space and a second memory space, the first memory space containing at least one system file; and
>
> at least one electronic data processor communicatively coupled to the network interface device and to the first and second memory space;
>
> the at least one electronic data processor configured to execute the first web browser process within the common operating system, wherein the first web browser process is capable of accessing data of a website via the network, accessing data contained in the first memory space and is further capable of initializing the second web browser process;
>
> the at least one electronic data processor further configured to execute the second web browser process within the common operating system, *wherein the second web browser process is capable of accessing data contained in the second memory space* and is further capable of generating data;
>
> the at least one electronic data processor further configured to pass data from the first web browser process to the second web browser process;
>
> wherein the portable computing and communication device is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second web browser process.

The specification discloses that a second processor may be unable to "initiate" access to a first memory:

> In a preferred embodiment, P2 140 is communicatively coupled to memory storage area M2 130, and *may be configured such that P2 140 is incapable of initiating access to memory storage area M1 110*.
>
> * * *
>
> In accordance with a preferred embodiment of the present invention, if any malware is downloaded from network 195, it is stored in memory 130, and/or run as a process on second processor 140. In the configuration of computer system 100, *any downloaded malware is rendered incapable of self initiating access to memory 110* or first processor 120, because second processor 140 is rendered incapable of initiating access to 110 and 120 without a direct or stored command from user 160. Any malware infection is thus confined.
>
> * * *
>
> A computer system 100 constructed in accordance with the principles of the present invention would be capable of disallowing a secure logical process, such

> as the second logical process described above, access to certain memory spaces, and/or disallowing a secure logical process from initiating access to another logical process. For example, the functions carried out by *P2 140 (FIG. 1) may comprise a secure logical process, which may be configured to be unable to automatically initiate access to either M1 110* or another logical process performing the functions of P1 120.

'247 Patent at 10:43-46, 11:38-46 & 16:34-43 (emphasis added).

During prosecution of the '247 Patent, the patentees distinguished the "Corthell" reference (United States Patent No. 6,192,477) as lacking a separate processor: "While Corthell does teach partitioning of the memory space into a primary partition (Figure 2, [block 204]) and a protected partition (Figure 2, [block 206]), he does not teach or suggest the partitioning of 'secure' and 'unsecure' instruction execution onto separate electronic data processors." (Dkt. No. 66, Ex. 3, 4/29/2008 Amendment Under 37 CFR §1.111 at 9 (square brackets in original); *see id.* at 10-12 ("Applicants' invention . . . does not rely on the user to have sufficient technical knowledge to determine the difference between malicious and non-malicious instructions.").)

On balance, Defendant has failed to identify any definitive statement by the patentees that the second web browser process can access data in *only* the second memory space. *See Omega Eng'g v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003) ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added); *id.* at 1325-26 ("[F]or prosecution disclaimer to attach, our precedent requires that the alleged disavowing actions or statements made during prosecution be both *clear and unmistakable*.") (emphasis added).

Although Defendant repeatedly emphasizes that its proposed architecture is necessary to be consistent with the security teachings of the specification, "[t]he fact that a patent asserts that an invention achieves several objectives does not require that each of the claims be construed as limited to structures that are capable of achieving all of the objectives." *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 908 (Fed. Cir. 2004). Also of note, above-quoted Claim 21 of the '500 Patent, for example, recites in part (emphasis added): "the portable computing and communication device is configured such that the *at least one system file residing on the first memory space is protected from corruption* by a malware process downloaded from the network and executing within the second web browser process."

Defendant's proposed construction is therefore hereby expressly rejected. No further construction is necessary. *See U.S. Surgical*, 103 F.3d at 1568 ("Claim construction is a matter of resolution of disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims, for use in the determination of infringement. It is not an obligatory exercise in redundancy."); *see also O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008) ("[D]istrict courts are not (and should not be) required to construe every limitation present in a patent's asserted claims."); *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1207 (Fed. Cir. 2010) ("Unlike *O2 Micro*, where the court failed to resolve the parties' quarrel, the district court rejected Defendants' construction.").

The Court accordingly hereby construes **"wherein the second web browser process is capable of accessing data contained in the second memory space"** to have its **plain meaning**.

C. "first memory space"

Plaintiffs' Proposed Construction	**Defendant's Proposed Construction**
"memory space accessible by the first web browser process, but not automatically accessible by the second web browser process"[6]	"memory space that is separate from and shares no common memory storage area with the second memory space"

[6] Plaintiffs previously proposed: "memory space accessible by the first web browser process, but not the second web browser process." (Dkt. No. 52, Ex. A at 9.)

(Dkt. No. 56 at 12; Dkt. No. 66 at 21.) Plaintiffs submit that this disputed term appears in all claims of the patents-in-suit. (Dkt. No. 56 at 12 n.24.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary construction: "memory space distinct from a second memory space."

Plaintiffs agreed with the Court's preliminary construction. Defendant expressed no direct opposition to the Court's preliminary proposal, but Defendant nonetheless maintained its proposal.

(1) The Parties' Positions

Plaintiffs argue that Defendant's proposed construction excludes disclosed embodiments and should therefore be rejected. (Dkt. No. 56 at 12.) Instead, Plaintiffs submit, "[t]he intrinsic evidence shows that the first memory space is any memory space accessible by the first web browser process, that is also not automatically accessible by the second web browser process." *Id.* Plaintiffs emphasize that the specification "defines the memory spaces by the level of access provided to each web browser process." (*Id.* at 14.) Finally, Plaintiffs argue that the specification "does not go so far as to state that the two memory spaces 'share no common memory storage area,'" and Plaintiffs cite Figure 9 as disclosing "an embodiment where the first and second memory spaces share common memory space but are separated logically." (*Id.*) Plaintiffs reiterate that the separation between the first memory space and the second memory space can be either physical or logical. (*Id.* at 15.)

Defendant responds that Plaintiffs' proposal of allowing overlap between the first and second memory spaces is contrary to the teaching in the specification of the "major problem" of trusted and untrusted programs "shar[ing] space on a common memory storage medium." (Dkt.

No. 66 at 21 (quoting ‘247 Patent at 6:56-60).) Defendant explains that “[i]f the memory spaces were not separate, malware could access the first memory space with the critical system and user files.” (*Id.* at 22.) Defendant submits that “[t]he specification discloses no embodiments where the first and second memory space overlap, and Plaintiffs offer no such intrinsic evidence.” (*Id.*) Defendant further submits that there is no disclosure “of how one would protect critical files in the first memory space if those files could also be part of the second memory space to which malware has access.” (*Id.*) Likewise, Defendant argues, “[i]f the memory spaces were overlapping, one could not erase the second memory space and restore it from critical files in the first memory space” as described in the specification. (*Id.* (citing ‘247 Patent at 12:46-14:2).) Finally, Defendant urges that Plaintiffs’ proposed constructions are “redundant in view of the accessing language already in the claims. The first and second ‘memory space’ terms are not the appropriate places to address the term ‘access.’” (*Id.* at 23.)

Plaintiffs reply that “Defendant never explains how sharing or overlap between the 1st and 2nd memory spaces is even possible under Plaintiffs’ construction. . . . If the second web browser process cannot [automatically] access the first memory space, then the memory spaces are separate by definition.” (Dkt. No. 67 at 3.) Plaintiffs argue that Defendant’s proposed construction is contrary to Figure 9, wherein “1st and 2nd memory spaces are separate, but may still share common memory storage area (such as the same drive).” (*Id.*)

<u>(2) Analysis</u>

Claim 44 of the ‘528 Patent recites, in relevant part (emphasis added):

> 44. A method of operating a portable computer capable of executing instructions using a common operating system and comprising a network interface device, at least a *first memory space* and a second memory space, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:

> exchanging data across a network of one or more computers with the network interface device and accessing at least one website;
>
> storing at least one system file in the *first memory space*;
>
> opening a first web browser process capable of accessing data of the at least one website via the network, wherein the first web browser process is capable of accessing data contained in the *first memory space*;
>
> opening a second web browser process, wherein the second web browser process is capable of accessing data contained in the second memory space, and is further capable of generating data for video display; and
>
> passing data from the first web browser process to the second web browser process;
>
> wherein the portable computer is configured such that the at least one system file residing on the *first memory space* is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

The Background section of the patents-in-suit states:

> A major problem faced by computer users connected to a network is that the network interface program (a browser, for example) is resident on the same processor as the O/S and other trusted programs, and shares space on a common memory storage medium. Even with security designed into the O/S, malware practitioners have demonstrated great skill in circumventing software security measures to create malware capable of corrupting critical files on the shared memory storage medium. When this happens, users are often faced with a lengthy process of restoring their computer systems to the correct configuration, and often important files are simply lost because no backup exists.
>
> Therefore, *what is needed in the art is a means of isolating the network interface program from the main computer system such that the network interface program does not share a common memory storage area with other trusted programs.* The network interface program may be advantageously given access to a separate, protected memory area, while being unable to initiate access to the main computer's memory storage area. With the network interface program constrained in this way, malware programs are rendered unable to automatically corrupt critical system and user files located on the main memory storage area. If a malware infection occurs, a user would be able to completely clean the malware infection from the computer using a variety of methods. A user could simply delete all files contained in the protected memory area, and restore them from an image residing on the main memory area, for example.

'247 Patent at 6:56-7:16 (emphasis added). The specification discloses:

> The first memory and data storage area 110 may comprise both volatile and nonvolatile memory devices, such as DRAMs and hard drives, respectively. Any

> memory structure and/or device capable of being communicatively coupled to P1 may be advantageously used in the present invention.

Id. at 9:48-57.

The specification further discloses that although a second process may not have automatic access to a first memory space, the second processor may access the first memory space if permission is granted:

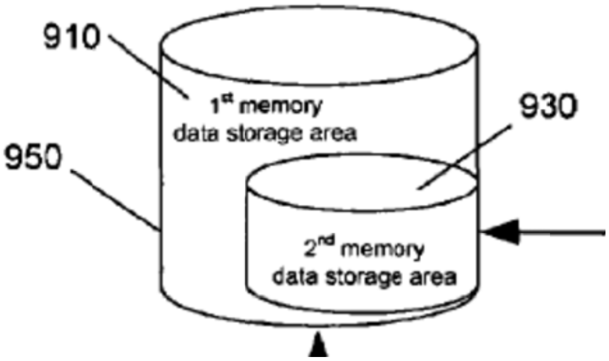
> The architecture of computer system 100 is designed to be capable of protecting memory 110 from malware initiated intrusions, and preventing malware from initiating unwanted processes on first processor 120. This is accomplished by using second processor 140 to isolate 110 and 120 from network 195. In a preferred embodiment, P2 140 is communicatively coupled to memory storage area M2 130, and may be configured such that P2 140 is incapable of initiating access to memory storage area M1 110. For example, *P2 140 may be capable of accessing memory storage area M1 110 with the strict permission of user 160*, either through a real time interaction or via stored configuration or commands. Such a configuration may be desirable in a multi-core or multi processor system, where user 160 may wish to use P2 140 in either a protected mode or an unprotected mode, depending on the application. However, user 160 is capable of denying P2 140 the capability of initiating access to memory storage area M1 110 without the user's permission.

Id. at 10:38-55 (emphasis added); *see id.* at 11:38-46 & 16:34-43.

As to separation between memory storage areas, the specification discloses:

> Additionally, memory areas 910 and 930 may comprise separate, isolated memory zones within a common physical memory space, such as separate partitions within the same hard drive, for example.

Id. at 16:44-47. Figure 9, cited by Plaintiffs, illustrates a "2nd memory data storage area 930" that appears to be located within a "1st memory data storage area 910." *See* '247 Patent at 16:17-19. The relevant portion of Figure 9 is reproduced here:



“The use of the terms ‘first’ and ‘second’ is a common patent-law convention to distinguish between repeated instances of an element or limitation.” *See 3M Innovative Props. Co. v. Avery Dennison Corp.*, 350 F.3d 1365, 1371 (Fed. Cir. 2003); *accord Free Motion Fitness, Inc. v. Cybex Int’l, Inc.*, 423 F.3d 1343, 1347 (Fed. Cir. 2005) (quoting *3M*).

Further, “[w]here a claim lists elements separately, the clear implication of the claim language is that those elements are distinct components of the patented invention.” *See Becton, Dickinson & Co. v. Tyco Healthcare Group, LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) (citations and internal quotation marks omitted).

On balance, however, although the memory spaces are distinct from one another (*see id.*), Defendant has failed to demonstrate that the “first memory space” must have “no common memory storage area” with the “second memory space.” In particular, Defendant has failed to establish that the “first memory space” must be physically separate from the “second memory space.” Defendant’s proposed construction is accordingly hereby expressly rejected.

The Court therefore hereby construes **“first memory space”** to mean **“memory space distinct from a second memory space.”**

D. “second memory space” and “second protected memory space”

“second memory space”	
Plaintiffs’ Proposed Construction	**Defendant’s Proposed Construction**
“memory space accessible by at least the second web browser process”	“memory space that is separate from and shares no common memory storage area with the first memory space”
“second protected memory space”	
Plaintiffs’ Proposed Construction	**Defendant’s Proposed Construction**
“protected memory space accessible by at least the second web browser process”	“protected memory space that is separate from and shares no common memory storage area with the first memory space”

(Dkt. No. 56 at 15-16; Dkt. No. 66 at 21.) Plaintiffs submit that the first of these disputed terms appears in all asserted claims of the ‘103, ‘500, and ‘528 Patents. Dkt. No. 56 at 15 n.30. Plaintiffs submit that the second of these disputed terms appears in all asserted claims of the ‘529 Patent. (*Id.* at 16 n.31.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary constructions: “second memory space” means “memory space distinct from a first memory space”; and “second protected memory space” means “protected memory space distinct from a first memory space.”

Plaintiffs agreed with the Court’s preliminary constructions. Defendant expressed no direct opposition to the Court’s preliminary proposal, but Defendant nonetheless maintained its proposals.

(1) The Parties' Positions

Plaintiffs present substantially the same arguments here as for the term "first memory space," addressed above, as to which Plaintiffs argue "the second memory space may also be accessed by the first web browser process." (Dkt. No. 56 at 16-17; *see* Dkt. No. 67 at 3.)

Likewise, Defendant's briefing addresses these disputed terms together with Defendant's arguments as to the term "first memory space," addressed above. (*See* Dkt. No. 66 at 21-23.)

(2) Analysis

Claim 44 of the '528 Patent recites, in relevant part (emphasis added):

> 44. A method of operating a portable computer capable of executing instructions using a common operating system and comprising a network interface device, at least a first memory space and a *second memory space*, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:
>
> . . .
>
> opening a second web browser process, wherein the second web browser process is capable of accessing data contained in the *second memory space*, and is further capable of generating data for video display; . . . .

The Summary of the Invention states:

> It is another object of the present invention to provide a computer system capable of executing instructions in a second logical process, wherein the second logical process is capable of accessing data contained in the second memory space, the second logical process being further capable of exchanging data across a network of one or more computers.
>
> * * *
>
> These objects and other advantages are provided by a preferred embodiment of the present invention wherein a computer system comprising a first electronic data processor is communicatively coupled to a first memory space and to a second memory space [and] a second electronic data processor is communicatively coupled to the second memory space and to a network interface device . . . .

'247 Patent at 8:1-6 & 8:32-38. The specification discloses:

> Communicatively coupled to P2 140 is second memory and data storage area 130 (M2), which may comprise any memory device or devices, such as the devices previously described as applicable to first memory 110.

Id. at 10:34-37.

On balance, as found above regarding the term “first memory space,” Defendant has failed to demonstrate that the “second memory space” must have “no common memory storage area” with the “first memory space.”

The Court accordingly hereby construes the disputed terms as set forth in the following chart:

Term	Construction
“second memory space”	**“memory space distinct from a first memory space”**
“second protected memory space”	**“protected memory space distinct from a first memory space”**

E. “the second electronic data processor is operating in a protected mode”

Plaintiffs’ Proposed Construction	**Defendant’s Proposed Construction**
No construction necessary; plain and ordinary meaning; the term is defined in the claim	“the second electronic data processor is configured such that it is incapable of initiating access to the first memory space”

(Dkt. No. 56 at 17; Dkt. No. 66 at 27.) Plaintiffs submit that this disputed term appears in Claims 1, 2, and 5 of the ‘528 Patent. (Dkt. No. 56 at 17 n.34.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary construction: “the second electronic data processor is configured such that it is incapable of automatically accessing the first memory space.”

Plaintiffs and Defendant agreed with the Court’s preliminary construction.

The Court therefore hereby construes **“the second electronic data processor is operating in a protected mode”** to mean **“the second electronic data processor is configured such that it is incapable of automatically accessing the first memory space.”**

F. “the at least one electronic data processor configured to execute the first web browser process within the common operating system, wherein the first web browser process is capable of accessing data of a website via the network, accessing data contained in the first memory space”

Plaintiffs’ Proposed Construction	**Defendant’s Proposed Construction**
Not indefinite; plain and ordinary meaning	Indefinite

(Dkt. No. 56 at 19.) Plaintiffs submit that this disputed term appears in all asserted claims of the patents-in-suit. (Dkt. No. 56 at 19 n.36.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with its preliminary construction that this disputed term is subsumed within Defendant’s below-discussed overall invalidity challenge. Neither side expressed any opposition to proceeding in such a fashion. Plaintiffs’ briefing as to this term is therefore addressed as part of addressing Defendant’s overall invalidity arguments, below.

G. “intelligent cellular telephone capability”

Plaintiffs’ Proposed Construction	**Defendant’s Proposed Construction**
Not indefinite No construction necessary; the term is defined in the claim limitation that it appears in	Indefinite

(Dkt. No. 56 at 24; Dkt. No. 66 at 14-16.) Plaintiffs submit that this disputed term appears in all asserted claims of the ‘500 Patent. (Dkt. No. 56 at 24 n.46.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary construction: "Plain meaning [Expressly reject Def[endant]'s indef[initeness] arg[ument]]."

(1) The Parties' Positions

Plaintiffs argue that Defendant "ignores the obvious which is that the term 'intelligent cellular telephone capability' is defined in the claim itself." (Dkt. No. 56 at 25.) Plaintiffs explain that the disputed term refers to "the capability a device receives with a secure web browser, including a first and second web browser process." (*Id.* at 26.)

Defendant responds that the disputed term, which was added during reissue prosecution and does not appear in the specification, has no commonly understood meaning and is not explained by the patents-in-suit. (Dkt. No. 66 at 14.) Defendant also submits that the disputed term "must be different from a 'smart phone', 'cellular data carrier network', or an 'intelligent cellular phone' because each of these devices was claimed separately. . . . [T]he Applicants did not explain to one of ordinary skill what an 'intelligent cellular telephone' was or how it was different from PDAs or smart phones." (*Id.*)

Defendant cites deposition testimony of inventor Alfonso Cioffi, as well as testimony of Plaintiffs' expert Dr. Dunsmore, that is purportedly inconsistent with Plaintiffs' current position that the disputed term "is defined by the remainder of the limitation in which it appears." (*Id.* at 14-15 (quoting Dkt. No. 56 at 25); *see* Dkt. No. 66, Ex. 26, 6/26/2014 Cioffi dep. at 228:20-229:10 (in response to question—"[w]ould you agree that persons skilled in the art that read these patents would understand that intelligent celepho -- excuse me, that intelligent cellular telephone capability to refer generally to the class of features that are found on higher end mobile phones" —stating that "it is possible that a person of skill in the art would come to that conclusion"); Dkt. No. 63, 6/9/2014 Dunsmore Decl. at ¶ 25 ("One of skill in the art at the time of the invention would understand intelligent cellular telephone capability to refer generally to the class of features that were found on higher-end mobile phones of that time such as web-browsing, reading and sending email, texting, GPS, cameras, and mobile applications.").)

Defendant concludes that although the claim language specifies one feature that must be included with an "intelligent cellular telephone capability" (namely a "secure web browser including a first web browser and a second web browser process"), "because there is no guidance in the intrinsic evidence as to what an ICTC [(intelligent cellular telephone capability)] is, the claim term is indefinite." (*Id.* at 16.)

Plaintiffs reply by reiterating that the disputed term refers to "the capability provided to 'a portable computer and communication device . . . using a wireless connection' when you add 'a secure web browser including a first web browser process and a second web browser process.'" (Dkt. No. 67 at 9.)

At the August 14, 2014 hearing, Defendant urged that the patents-in-suit and their prosecution histories perhaps demonstrate what an intelligent cellular telephone capability is *not* but do not set forth what it *is.*

(2) Analysis

The Supreme Court of the United States has recently "read [35 U.S.C.] § 112, ¶ 2 to require that a patent's claims, viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2129 (2014). "A determination of claim indefiniteness is a legal conclusion that is drawn from the court's performance of its duty as the construer of patent claims." *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1347

(Fed. Cir. 2005) (citations and internal quotation marks omitted), *abrogated on other grounds by Nautilus*, 134 S.Ct. 2120.

The specification contains no disclosures regarding any "intelligent" device, let alone any "intelligent cellular telephone capability." Plaintiffs have cited deposition testimony in which inventor Alfonso Cioffi referred to surrounding claim language:

> Q . . . Can you tell me what you mean by intelligent cellular phone capability?
> A It is a capability that is -- that is realized when coupled with a secure web browser process including a first web browser process and a second web browser process. That -- that -- that statement -- that -- I mean, I guess, in the termin[a]l -- that limitation, that is all one statement.
> Q Well, again --
> A That -- that -- that's all together.
> Q I'm just asking for you, if you will, describe what you mean in the patent by intelligent cellular telephone capability.
> A We mean the capability along with the rest of the words in that phrase. I mean, that's -- that's -- that's -- that's -- that's a standalone phrase. Those words always appear together in the way we use it. We choose -- we chose to define it that way.

(Dkt. No. 57-1, 6/26/2014 Cioffi dep. at 225:16-226:9.) Inventor testimony, however, is of limited weight. *Howmedica Osteonics Corp. v. Wright Med. Tech., Inc.*, 540 F.3d 1337, 1346-47 (Fed. Cir. 2008) (noting that inventor testimony is of limited weight because "an inventor understands the invention but may not understand the claims, which are typically drafted by the attorney prosecuting the patent application").

During prosecution of the '500 Patent, for example, the examiner rejected claims based on the "Narin" reference (United States Patent Application Publication No. 2002/0002673):

> . . . Narin teaches a portable computing and communication device capable of executing instructions using a common operating system, comprising:
>
> . . .
>
> a cell phone communication capability (paragraph 0022, cellular networks use RF, or radio frequency) . . . .

(Dkt. No. 66, Ex. 13, 6/13/2011 Office Action at ¶ 11; *see id.* at ¶¶ 19, 29, 37 & 42 (similar)); *see also* Narin at ¶ 22 ("By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media.").

In response, the patentees introduced the term "intelligent cellular telephone capability" (additions underlined and deletions in strikethrough or double square brackets, as in original):

> 21. (Currently Amended) A portable computing and communication device capable of executing instructions using a common operating system, comprising:
>
> a network interface device configured to exchange data across a network of one or more computers using a wireless connection;
>
> ~~a cell phone communication capability~~an intelligent cellular telephone capability with a secure web browser including a first browser process and a second browser process;
>
> at least a first memory space and a second memory space, the first memory space containing at least one system file; and
>
> at least one electronic data processor communicatively coupled to a network interface device and to the first and second memory space;
>
> the at least one electronic data processor configured to execute [[a]]the first browser process within the common operating system, wherein the first browser process is capable of accessing data contained in the first memory space and is further capable of initializing [[a]]the second browser process;
>
> the at least one electronic data processor further configured to execute the second browser process within the common operating system, wherein the second browser process is capable of accessing data contained in the second memory space and is further capable of generating data;
>
> the at least one electronic data processor further configured to pass data from the first browser process to the second browser process;
>
> wherein the portable computing and communication device is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process.

(Dkt. No. 66, Ex. 14, 10/13/2011 Amendment Under 37 CFR §1.111 at 24; *see also id.* at 27 & 30.) Further, the patentees stated:

> As the Examiner correctly points out, Narin does mention that computer 110 includes computer readable media having communication media with wireless media such as radio frequency ("RF"). (Paragraph [0022].) This is a simple listing of well known wireless media and *does not teach an intelligent cellular*

> *telephone capability with a built-in secure web browser*. Moreover, there is no affirmative statement in Narin that the portable computing and communication device includes the *intelligent cellular telephone capability with the secure web browser*. Narin is merely silent on the concept.

Id. at 18 (emphasis added).

In response, the examiner cited the "Toedtli" reference (U.S. Patent Application Publication No. 2002/0052809) as disclosing an "intelligent cellular phone":

> 17. Narin does not teach an intelligent cellular telephone capability with a secure web browser.
>
> 18. Toedtli teaches wherein the portable computer comprises an *intelligent cellular phone* with a secure web browser (paragraphs 0030-0031, a cellular phone with a WAP [(Wireless Application Protocol)] browser that establishes a secure connection to the web server and can provide cryptographically encoded data).
>
> 19. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the secure application of Narin to be a secure web browser operating on an *intelligent cellular phone* network, since Toedtli states at paragraph 0030 that the WAP browser provides a secure connection and can cryptographically encode data, thereby making any transactions occurring from the cell phone more secure.

(*Id.*, Ex. 17, 11/17/2011 Office Action at ¶¶ 17-19;[7] *see* Dkt. No. 63, 6/9/2014 Dunsmore Decl. at 14 n.4 ("Wireless Application Protocol (WAP) is a technical standard for accessing

[7] Paragraph 30 of Toedtli discloses:

> In a further embodiment, the buyer can use the internet 9 for contacting the database holder, either by using a cellular phone with browsing capabilities (such as WAP), or by using a computer 10*c*. In both cases, the buyer contacts a secure web server 8 of the database holder, which queries him for the article number and the phone number. Secure web server 8 is able to establish a secure connection to computer 10*c* or cellular phone 10*a*, which connection positively identifies at least the server (and preferably the client) and provides cryptographically encoded data exchange between them, e.g. by using known methods involving asymmetric public and private key pairs.

information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones that use the protocol.”).)

The examiner’s use of the disputed term without objection suggests that the surrounding claim language provides sufficient context. *See Am. Hoist & Derrick Co. v. Sowa & Sons, Inc.*, 725 F.2d 1350, 1359 (Fed. Cir. 1984) (patent examiners are “assumed . . . to be familiar from their work with the level of skill in the art”), *abrogated on other grounds*, *Therasense, Inc. v. Becton, Dickinson & Co.*, 649 F.3d 1276 (Fed. Cir. 2011); *see also PowerOasis, Inc. v. T-Mobile USA, Inc.*, 522 F.3d 1299, 1304 (Fed. Cir. 2008) (citing *American Hoist*); *Salazar v. Procter & Gamble Co.*, 414 F.3d 1342, 1347 (Fed. Cir. 2005) (“Statements about a claim term made by an Examiner during prosecution of an application may be evidence of how one of skill in the art understood the term at the time the application was filed.”).

On one hand, “claims are interpreted with an eye toward giving effect to all terms in the claim.” *Digital-Vending Servs. Int’l, LLC v. Univ. of Phoenix, Inc.*, 672 F.3d 1270, 1275 (Fed. Cir. 2012) (quoting *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006)). This proposition, as a general matter, disfavors Plaintiffs’ proposal that the disputed term is defined by other claim language.

On the other hand, “surplusage may exist in some claims.” *Decisioning.com, Inc. v. Federated Dep’t Stores, Inc.*, 527 F.3d 1300, 1312 n.6 (Fed. Cir. 2008); *accord ERBE Elektromedizin GmbH v. Canady Tech. LLC*, 629 F.3d 1278, 1286 (Fed. Cir. 2010).

On balance, the best reading of the claim language and the prosecution history is that the “intelligent cellular telephone capability” is provided by the use of “a secure web browser including a first web browser process and a second web browser process,” as recited in the claims. The surrounding claim language thus renders the scope of the disputed term "reasonabl[y] certain[]." *Nautilus*, 134 S. Ct. at 2129; *see Trover Group, Inc. v. Tyco Int'l, Ltd.*, No. 2:13-CV-52, 2014 WL 3736340 (E.D. Tex. July 28, 2014) (Bryson, J.) ("Although the term 'amplitude' is used only in the claims and is not defined or discussed in the specification, the Court does not find it to be indefinite. To the contrary, the context makes the meaning of the term sufficiently clear to ensure that the term is not so indefinite as to invalidate the claims in which it appears.").

Defendant's indefiniteness argument is therefore hereby expressly rejected. No further construction is necessary. *See U.S. Surgical*, 103 F.3d at 1568; *see also O2 Micro*, 521 F.3d at 1362.

The Court accordingly hereby construes **"intelligent cellular telephone capability"** to have its **plain meaning**.

H. "critical file"

Plaintiffs' Proposed Construction	**Defendant's Proposed Construction**
Not indefinite "files that are required to start or run the computer's systems properly"[8]	Indefinite

(Dkt. No. 56 at 28; Dkt. No. 66 at 16-18.) Plaintiffs submit that this disputed term appears in Claim 21 of the '103 Patent. (Dkt. No. 56 at 28 n.28.)

Shortly before the start of the August 14, 2014 hearing, the Court provided the parties with the following preliminary construction: "Indefinite [Claim 21 of the '103 Patent is invalid]."

[8] Plaintiffs previously proposed: "Files that are required to start or run the operating system properly." Dkt. No. 52, Ex. A at 16.

(1) The Parties' Positions

Plaintiffs rely upon the opinion of their expert that a "critical" file is well understood by persons of ordinary skill in that art and that the specification is consistent with that understanding. (*See* Dkt. No. 56 at 28-29.) Plaintiffs submit that the claim is clear because "[o]ne of skill can easily determine if a file is critical: if the file can be removed or modified without interfering with the proper operation of the computer's software systems then it is not critical." (*Id.* at 29.) Further, Plaintiffs argue that the disclosure, in the specification, of "critical user files" does not render the term "critical file" indefinite because "a user file in some rare instances could be a critical file provided the particular user file was required to start or run the computer's systems properly." (*Id.*)

Defendant responds that "the specification and the file history teach that critical files include critical user, system and application files." (Dkt. No. 66 at 17.) Defendant submits that "[b]ecause 'critical file' includes user files, it is an entirely subjective term that depends on the viewpoint of the particular user." (*Id.*) Defendant concludes that because "the specification does not set forth an objective standard to determine the scope of 'critical file,'" this claim term is indefinite. (*Id.* at 17-18.)

Plaintiffs reply:

> Defendant's entire argument that "critical file" is indefinite rests on the sole basis that a critical file must also include a user file because in three instances (out of more than 20), the specification makes reference to "critical user files." As explained in Plaintiffs' Opening Brief, one of skill would not view three stray references to "critical user files" as changing the otherwise well understood definition of "critical file" by one of ordinary skill. Indeed, both [side's] experts agree that "critical files" are synonymous with "system files." [Dkt. No. 56] at 28.

(Dkt. No. 67 at 10.) Plaintiffs emphasize that "a clear and ordinary meaning is not properly overcome (and a relevant reader would not reasonably think it overcome) by a few passing references that do not amount to a redefinition or disclaimer." (*Id.* (quoting *Ancora Techs. v. Apple, Inc.*, 744 F.3d 732, 737 (Fed. Cir. 2014)).)

At the August 14, 2014 hearing, Plaintiffs reiterated that the numerous references in the specification to "critical" system files vastly outweigh the three stray references to "critical" user files.

<u>(2) Analysis</u>

As a threshold matter, although the Court can consider expert opinions submitted by the parties, such evidence is extrinsic and carries less weight than the intrinsic evidence. *See Phillips*, 415 F.3d at 1318.

Claim 21 of the '103 Patent recites:

> 21. A portable computer based system capable of executing instructions using a common operating system and protect[ing] *critical files* from malicious attacks via a network of one or more computers, comprising:
>
> a first logical process capable of executing instructions within the common operating system using at least one electronic data processor and further capable of accessing a first memory space, wherein the first memory space contains at least one *critical file*; and
>
> at least one secure browser process capable of executing instructions within the common operating system using the at least one electronic data processor and further capable of accessing a second memory space;
>
> the first logical process configured to:
>
> accept data entry from a computer user;
> initialize the at least one secure browser process; and
> pass data to the at least one secure browser process;
>
> the at least one secure browser process configured to:
>
> execute instructions from a process potentially containing malware downloaded from the network of one or more computers;
> access data contained in the second memory space, wherein the process potentially containing malware is capable of accessing the second memory space but is denied access to the first memory space;
> store at least one temporary internet file on the first or second memory space;

> block the process potentially containing malware from modifying search requests when accessing a search engine; and
>
> generate website video data for display;
>
> wherein the portable computer based system is configured such that the at least one *critical file* residing on the first memory space is protected from corruption by the process potentially containing malware downloaded from the network and executing as part of the at least one secure browser process;
>
> wherein the portable computer based system is configured such that the at least one temporary internet file is automatically deleted upon closing the at least one secure browser process.

The claim thus does not define or illuminate any objective distinction between a "critical file" and a mere "file."

"[W]hen faced with a purely subjective phrase . . ., a court must determine whether the patent's specification supplies some standard for measuring the scope of the phrase." *Datamize*, 417 F.3d at 1351, *abrogated on other grounds by Nautilus*, 134 S.Ct. 2120. The specification discloses:

> An aspect of some current computer architectures that has contributed to the security problem is that by default programs are typically allowed to interact with and/or alter other programs and data files, including *critical operating system files*, such as the [W]indows [R]egistry, for example.
>
> * * *
>
> Security holes in *critical applications* are discovered quite often, and just keeping up with all the patches is cumbersome.
>
> * * *
>
> Therefore, what is needed in the art is a means of isolating the network interface program from the main computer system such that the network interface program does not share a common memory storage area with other trusted programs. The network interface program may be advantageously given access to a separate, protected memory area, while being unable to initiate access to the main computer's memory storage area. With the network interface program constrained in this way, malware programs are rendered unable to automatically corrupt *critical system and user files* located on the main memory storage area.
>
> * * *

> It is an object of the present invention to provide a computer system capable of preventing malware programs from automatically corrupting *critical user and system files*.
>
> * * *
>
> It is another object of the present invention to provide a user with an easy and comprehensive method of restoring *critical system and user files* that may have been corrupted by a malware infection.
>
> * * *
>
> Second processor 140 and memory 130 act as a separate computer system, interacting with network 195 while isolating network 195 from the first processor 120 and memory 110. Memory 130 may store *critical application and system files* required by second processor 140 to execute the desired tasks.

’247 Patent at 3:39-44, 6:45-47, 7:1-11, 7:42-44, 7:53-56 & 11:11-16. These are not merely "passing references," as Plaintiffs argue. Dkt. No. 67 at 10 (quoting *Ancora*, 744 F.3d at 738). Instead, the above-quoted passages disclose that in addition to "system" files being critical, "user" files can be critical as well. Similarly, during prosecution of the ‘247 Patent, the patentees stated:

> If malicious instructions are executed within the second logical process, any data corruption is confined to the second electronic memory space. *Critical user data* residing on the first electronic memory space is thereby protected from corruption by a malicious (malware) process downloaded from the network and executing on the second logical process.

Id., Ex. 3, 4/29/2008 Amendment Under 37 CFR §1.111 at 11 (emphasis added).

The specification and the prosecution history thus tend to confuse rather than clarify the meaning of "critical file" because whereas what is critical to operation of the computer system may be objectively determinable, what is critical to a user may be entirely subjective.

As to the experts' opinions, on one hand Defendant's expert acknowledges: "A person of ordinary skill in the art knows that 'system files' are synonymous with 'critical file' and 'critical system file.'" (*See* Dkt. No. 66, Ex. 23, 7/10/2014 Arbaugh Decl. at 32.)

On the other hand, although Plaintiffs' expert maintains that a user file cannot be a "critical" file, Plaintiffs' expert acknowledges that what is "critical" to a user is subjective. *See* (Dkt. No. 63, 6/9/2014 Dunsmore Decl. at ¶ 35 ("One of skill would understand that a critical file would not be a user file, as users may disagree what is and is not critical to them. A user may have files containing information such as accounts and passwords, bank account numbers, credit card numbers, etc. that a user may consider as 'critical user files.'").) Defendant's expert agrees that "a 'critical user file' is entirely subjective because what is critical to one person may not be critical to another." (*See* Dkt. No. 66, Ex. 23, 7/10/2014 Arbaugh Decl. at 32.)

Plaintiffs propose to give clear meaning to the disputed term by construing it to mean "files that are required to start or run the computer's systems properly." To whatever extent Plaintiffs are proposing a "narrowing construction," as contemplated by the *Exxon* case, *Nautilus* abrogated *Exxon* in this regard and thereby eliminated any such avenue of avoiding an indefiniteness finding. *See Exxon Research & Eng'g Co.*, 265 F.3d 1371, 1375 (Fed. Cir. 2001) ("If a claim is insolubly ambiguous, and no narrowing construction can properly be adopted, we have held the claim indefinite."), *abrogated by Nautilus*, 134 S.Ct. at 2124, 2130 n.9.

In sum, because "critical file" is a subjective term, and because neither the specification nor the prosecution history sets forth any standard for measuring the scope of that term, the Court concludes that the term "critical file" fails to "inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus*, 134 S. Ct. at 2129; *see Datamize,* 417 F.3d at 1351.

The Court accordingly hereby finds that the term **"critical file"** is **indefinite** and that **Claim 21 of the '103 Patent is therefore invalid**.

I. Defendant's 35 U.S.C. § 112, ¶ 2 Invalidity Arguments as to All Asserted Claims

Defendant argues that the asserted claims are invalid pursuant to 35 U.S.C. § 112, ¶ 2 for two reasons. First, Defendant argues that all of the asserted claims are contrary to the specification because the "core security teaching" set forth in the specification requires isolating the network interface program so that it does not have access to files stored in the first memory space. (*See* Dkt. No. 66 at 6-12 (discussing *Allen Eng'g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1348-49 (Fed. Cir. 2002)).) Second, Defendant argues that by eliminating the requirement of two physically separate processors, 40 of the 45 asserted claims "fail to include the physical hardware separation the applicants told the Patent Office their original invention required." (*Id.* at 12 (capitalization modified); *see id.* at 12-13 (citing *Allen Eng'g*, 299 F.3d at 1348-49).)

As background, 35 U.S.C. § 112, ¶ 2 states:[9]

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

This statute contains two distinct requirements. One is known as the "definiteness" requirement, which has been asserted by Defendant as to the terms "intelligent cellular telephone capability" and "critical file," discussed above. The other is the "regards as his invention" requirement, which is distinct from definiteness. *See Ancora*, 744 F.3d at 739. Defendant argues that all of the asserted claims fail to satisfy this second requirement. "The determination whether

[9] The Leahy-Smith America Invents Act ("AIA") amended this statute so as to read: "The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention." It appears that the pre-AIA version applies to the patents-in-suit. Regardless, the amendment would have no effect on the Court's analysis in the present case.

a claim recites 'the subject matter which the applicant regards as his invention,' like a determination whether a claim is sufficiently definite, is a legal conclusion that is drawn from the court's performance of its duty as the construer of patent claims." *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1377 (Fed. Cir. 2000) (citation and internal quotation marks omitted).

(1) Contradicting the "Core Security Teaching" of the Specification

(a) The Parties' Positions

Plaintiffs argue: "[T]he asserted claims can be logically reconciled with the specification because it discloses examples of the very embodiments claimed. In Figure 1 of the common specification for the patents-in-suit, the first web browser process (represented by P1) is directly connected to the network interface device through the two-way communication link 191." (Dkt. No. 56 at 20.) Plaintiffs submit that Defendant's expert fails to address this disclosure. (*Id.* at 23.) Plaintiffs explain that "one of skill in the art knows there are low threat tasks involving communication with the network – such as passing encryption and decryption keys (*see, e.g.*, ['247 Patent at] 17:42-44), accessing secure websites with digital certificates, and streaming bits from a network to a media player – that can be carried out with a high level of confidence." (*Id.*) Plaintiffs also submit a declaration by their own expert. (*See* Dkt. No. 63, 6/9/2014 Dunsmore Decl. at ¶¶ 14-21.)

Further, Plaintiffs urge that "one of skill in the art would recognize that the fundamental nature of the invention allows, but does not require, the first logical process to be isolated from the network." (Dkt. No. 56 at 22.) Plaintiffs submit that "as explained by Professor Dunsmore [(Plaintiffs' expert)], the first logical process could simply act as a pass-through and allow *all* the data received from the network interface to flow to the second logical process for execution and eliminate the entire basis of Defendant's criticism that the first logical process may be exposed to malware by having a network connection." (*Id.* at 23.)

Plaintiffs conclude that "the requirement that all the asserted claims of the patents-in-suit have a first web browser process with a connection to the Internet is entirely consistent with the common specification, while it is also apparent to one [of] skill in the art that having such a connection is well within what the patentees regarded as their invention." (*Id.* at 24; *see id.* at 5-6 (citing *Ancora*, 744 F.3d at 739 (distinguishing *Allen Eng'g*); citing *Imperium (IP) Holdings, Inc. v. Apple, Inc.*, 920 F. Supp. 2d 747, 763-65 (E.D. Tex. 2013) (Clark, J.) (adopting report and recommendation rejecting argument that claims were inconsistent with the specification)).)

Defendant responds that all of the asserted claims are invalid because "[the] reissued claims . . . contradict the core security teaching of the original patent specification, which required isolating the network interface program so that it did not have access to the critical files stored in the first memory space." (Dkt. No. 66 at 6; *see id.* at 5-6 (citing *Allen Eng'g*, 299 F.3d at 1348-49; citing *Juxtacomm-Texas Software, LLC v. Axway, Inc.*, No. 6:10-cv-11, 2012 WL 7637197, at *4-*5 (E.D. Tex. July 5, 2012) (Davis, J.) (discussing *Allen Eng'g*), *aff'd*, No. 2013-1004, -1025, 532 F. App'x 911 (Fed. Cir. Sept. 30, 2013); citing *Tech. Innovations, LLC v. Amazon.com, Inc.*, Civ. No. 11-690, 2014 WL 1292093, at *4-*5 (D. Del. Mar. 31, 2014) (Robinson, J.) (discussing *Allen Eng'g*)).)

Defendant explains: "The specification does not disclose *any* embodiment with a network interface program, much less a web browser program, having access to the first memory space containing the trusted content. Moreover, *nowhere* in the specification is it explained how trusted content on the first memory space would be protected if the network interface program, or web browser, has access to the first memory space." (Dkt. No. 66 at 7.) Defendant submits:

> [The] [reissue] claims now require a first process to access both the "first memory space" where critical files are stored and "data of a website via the network." This addition undermines the core "isolation" principle of the invention (which was used to distinguish prior art in the '247 patent file history) because the first process is now capable of accessing data from a website via a network and *also* capable of accessing the "first memory space."

(*Id.* at 7-8.) Finally, Defendant argues that the use of "communication link 191," shown in Figure 1, does not support the reissue claims because communication link 191 is disclosed only as being used for sending decryption keys. (*Id.* at 10.) Defendant argues that "[b]ecause the decryption keys bypass the second processor, malware cannot steal the decryption keys and access the sensitive data." (*Id.*)

Plaintiffs reply that "[i]n reissue, the inventors narrowed the original claims to specify that the first logical process must also be at least 'capable' of accessing the Internet." (Dkt. No. 67 at 4.) Plaintiffs also reiterate their opening arguments, particularly as to the disclosure of communication link 191. (*Id.* at 5-7.) For example, Plaintiffs argue that "one of skill would know, and the patent teaches, in order to carry out tasks such as encrypted online internet banking, the first web browser process can be used to carry out a trusted activity with the Internet, while the second process is used to run programs and render web pages potentially containing malware." (*Id.* at 6 (citing Ex. L, 6/17/2014 Dunsmore dep. at 185:22-187:25).) Plaintiffs conclude that "[u]nlike Defendant's cited cases, the claims are drafted as the inventors intended, and they are drafted consistent with one or more disclosed embodiments in the patents' specification." (Dkt. No. 67 at 7.)

At the August 14, 2014 hearing, Defendant reiterated that Plaintiffs' reliance on communication link 191 must fail because there is no disclosure of that link being used to transfer *data* to or from the network, only decryption keys. Defendant also urged that there is no support in the intrinsic evidence for Plaintiffs' expert's discussion of allowing a first processor to access the network so as to conduct "low risk" activities or to "pass through" information to a second processor. Plaintiffs replied that their expert opined as to what a person of ordinary skill in the art at the relevant time would have understood from the specification.

(b) Analysis

"Where it would be apparent to one of skill in the art, based on the specification, that the invention set forth in a claim is not what the patentee regarded as his invention, we must hold that claim invalid under § 112, paragraph 2." *Allen Eng'g*, 299 F.3d at 1349 ("it is apparent from a simple comparison of the claims with the specification that the inventor did not regard a trowel in which the second gear box pivoted only in a plane perpendicular to the biaxial plane to be his invention"; "the specification describes this structure in contrary terms, stating that 'rotation about the axis established by bolt 272 is not permitted; gearbox 85A cannot pivot in a plane perpendicular to the biaxial plane'"; "we conclude as a matter of law that [the] claims . . . which include the incorrect 'perpendicular' limitation[] are invalid under § 112, paragraph 2"). Also, the *Juxtacomm* case cited by Defendant found that "there must be a showing of a logical inconsistency or contradiction between the claims and the specification." *Juxtacomm*, 2012 WL 7637197, at *4 (discussing *Allen Eng'g*).

Claim 21 of the '500 Patent is representative and recites (emphasis added):

> 21. A portable computing and communication device capable of executing instructions using a common operating system, comprising:
>
> a network interface device configured to exchange data across a network of one or more computers using a wireless connection;
>
> an intelligent cellular telephone capability with a secure web browser including a first web browser process and a second web browser process;
>
> at least a first memory space and a second memory space, the first memory space containing at least one system file; and
>
> at least one electronic data processor communicatively coupled to the network interface device and to the first and second memory space;
>
> the at least one electronic data processor configured to execute the first web browser process within the common operating system, *wherein the first web*

> *browser process is capable of accessing data of a website via the network, accessing data contained in the first memory space* and is further capable of initializing the second web browser process;
>
> the at least one electronic data processor further configured to execute the second web browser process within the common operating system, wherein the second web browser process is capable of accessing data contained in the second memory space and is further capable of generating data;
>
> the at least one electronic data processor further configured to *pass data from the first web browser process to the second web browser process*;
>
> wherein the portable computing and communication device is configured such that the *at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second web browser process*.

The claim thus recites that even though the first web browser process has network access, data can be passed to a second web browser process, and "at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and *executing within the second web browser process*."

Moreover, as Plaintiffs have noted, the specification discloses: "Decryption keys may be passed between P1 120 and the network interface device 190 via the communication link 191." *See* '247 Patent at 17:42-44. The "communication link 191" is illustrated in Figure 1 as a connection between "1st processor 120" and "Network interface 190." Figure 1 is reproduced here:

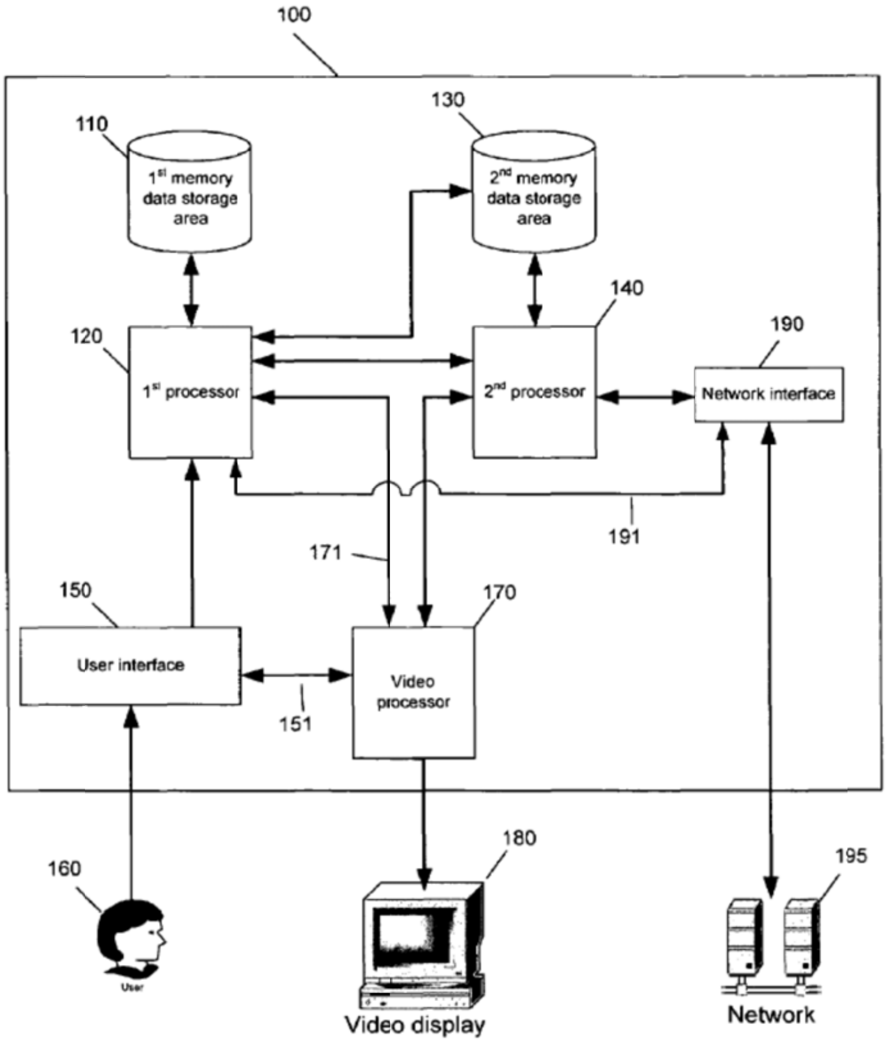


Fig. 1

Though perhaps not dispositive, this disclosure is probative. *See Vitronics*, 90 F.3d at 1582-83 (noting that a claim interpretation in which the only embodiment or a preferred embodiment "would not fall within the scope of the patent claim . . . is rarely, if ever, correct and would require highly persuasive evidentiary support"). Plaintiffs' expert, Dr. Dunsmore, has provided further explanation through deposition testimony:

> Q. Does the specification[] teach a person of ordinary skill that the decryption keys are actually passed into the network?

> A. It doesn’t say that explicitly, but having a network interface, the very terminology interface suggests that it is going to be something that’s going to exchange information with the network. From a pragmatic standpoint if I am one of the skill and I realize, for example, if I am doing internet banking and back in processor 120 I want to send my account and password, I want to encrypt that, and so certainly if I send an encryption key followed by the encrypted text, it has got to go further than just the network interface or I do not accomplish my internet banking.
>
> * * *
>
> Q. And so your belief is looking at lines 42 to 44 of column 17 is that the encryption keys will actually be sent over the network in addition to the encrypted data?
>
> A. That is certainly my expectation.

(Dkt. No. 57-2, 6/17/2014 Dunsmore dep. at 120:19-121:9 & 121:14-19.) Although such expert testimony carries less weight than the intrinsic evidence, expert opinions can be considered. *See Phillips*, 415 F.3d at 1318; (*but see* Dkt. No. 66, Ex. 25, 6/17/2014 Dunsmore dep. at 250:7-20 (“I am an expert in software engineering and certainly with web browsers and so on. I am not an expert in computer security. . . . I do not view myself as an expert in malware protection. I am aware of the dangers of malware. I am aware of the fact that it can be -- that it can be infected via web browsers, but I am certainly not an expert in that.”).)

On balance, Defendant has failed to demonstrate any logical inconsistency or contradiction between the claims and the specification. Of particular note, in the *Allen Engineering* case relied upon by Defendant the patentee agreed that the claims were inconsistent with the specification because of a claim drafting error. 299 F.3d at 1349; *see Ancora*, 744 F.3d at 739 (“[T]his case is unlike *Allen*, where the patentee agreed that the claim language did not match what he regarded as his invention, as the intrinsic record unambiguously showed, and this court denied the patentee’s request to reject the claim language’s clear, ordinary meaning. Here, Ancora embraces the claim language’s clear, ordinary meaning, and for the reasons we have explained, we do not think that the specification and prosecution history establish that the applicants regarded their invention as something contrary to that meaning.”).

Finally, any remaining arguments concerning lack of support in the specification pertain to the requirements of enablement or written description (or pertain to the prohibition against “new matter” or the rule against “recapture,” which are discussed below) and are thus not addressed by the present claim construction proceedings. *See Phillips*, 415 F.3d at 1327 (“[W]e have certainly not endorsed a regime in which validity analysis is a regular component of claim construction.”).

The Court accordingly rejects Defendant’s invalidity argument.

(2) Physically Separate Processors

(a) The Parties’ Positions

Defendant argues that 40 of the 45 asserted reissue claims are invalid because the new claims “eviscerate[] the physical hardware separation that the Applicants relied on to convince the Patent Office to issue their original claims.” (Dkt. No. 66 at 12.)

Plaintiffs reply that “Figure 9 and column 16 indisputably teach embodiments using a single processor.” (Dkt. No. 67 at 8 (citing ‘528 Patent at 16:10-12 (‘247 Patent at 16:22-24)).)

(b) Analysis

The Background section of the specification states:

> Therefore, what is needed in the art is a means of isolating the network interface program from the main computer system such that the network interface program does not share a common memory storage area with other trusted programs. The network interface program may be advantageously given access to a separate, protected memory area, while being unable to initiate access to the main computer’s memory storage area. With the network interface program constrained in this way, malware programs are rendered unable to automatically corrupt critical system and user files located on the main memory storage area.

‘247 Patent at 7:1-11.

During prosecution of the ‘247 Patent, the patentees stated:

> Corthell [(United States Patent No. 6,192,477)] teaches the use of a computer system using a single electronic data processor (Figure 1, [block 102]), utilizing a redirector (Figure 2, [block 214]) and filter (Figure 2, [block 216]) mechanism to protect against attacks by malware. Corthell, therefore, teaches the use of a single electronic data processor that is necessarily executing all instructions, including those related to: (1) the operating system, (2) “unsecure” operations, such as a browser program (column 5, lines 5-8), and (3) a software based redirector and filter mechanism (column 5, lines 65-68). While Corthell does teach partitioning of the memory space into a primary partition (Figure 2, [block 204]) and a protected partition (Figure 2, [block 206]), he does not teach or suggest the partitioning of “secure” and “unsecure” instruction execution onto *separate electronic data processors*.
>
> In stark contrast, Applicants teach the use of a *multi-processor* computer having at least a *first and second electronic data processor* capable of executing instructions using a common operating system. The second electronic data processor is capable of being configured in a protected mode when a network process is active. Such a configuration allows for a *physical hardware separation or partitioning of instruction execution on physically separate processors (or processor cores)*, in contrast to Corthell’s teaching of executing all instructions on a single electronic data processor. By *physically separating the execution of trusted instructions* (the operating system running on the first electronic data processor, for example) *from untrusted network process instructions* (a Java script downloaded from the internet, for example), a higher level of security may be achieved.

(Dkt. No. 66, Ex. 3, 4/29/2008 Amendment Under 37 CFR §1.111 at 9-10 (citation omitted; emphasis added; square brackets in original).)

Here, unlike Defendant’s “regards as his invention” argument regarding the first web browser process having network access (discussed above), Defendant appears to be arguing that the reissue claims violate the prohibition against “new matter” or the rule against “recapture” (or both). *See* 35 U.S.C. § 251; *see generally Revolution Eyewear, Inc. v. Aspex Eyewear, Inc.*, 563 F.3d 1358, 1366-68 (Fed. Cir. 2009) (discussing “new matter” and “recapture”); *In re Clement*, 131 F.3d 1464, 1468 (Fed. Cir. 1997) (“The recapture rule . . . prevents a patentee from regaining through reissue the subject matter that he surrendered in an effort to obtain allowance of the original claims. Under this rule, claims that are broader than the original patent claims in a manner directly pertinent to the subject matter surrendered during prosecution are impermissible.") (citations and internal quotation marks omitted).

General claim construction proceedings are not the proper vehicle for resolving such disputes. *See MBO Labs., Inc. v. Becton, Dickinson & Co.*, 602 F.3d 1306, 1312, 1314 (Fed. Cir. 2010) (reviewing grant of summary judgment of invalidity based on recapture, noting that "[w]e review a district court's legal determination that a reissue patent violates the rule against recapture without deference"; noting that the first step in applying the rule against recapture is to construe the reissued claims); *see also Hester Indus., Inc. v. Stein, Inc.*, 142 F.3d 1472, 1479 (Fed. Cir. 1998) (reviewing grant of summary judgment that asserted reissue claims were invalid for failing to meet requirements of 35 U.S.C. § 251; noting that "[w]hether the statutory requirements of 35 U.S.C. § 251 have been met is a question of law," but "[t]his legal conclusion can involve underlying factual questions") (citation omitted); *cf. Brooktree Corp. v. Advanced Micro Devices, Inc.*, 977 F.2d 1555, 1574 (Fed. Cir. 1992) (upon review of jury finding that an addition was not "new matter" prohibited by 35 U.S.C. § 132, noting that "[t]he question whether new matter has been added to an application is a question of fact"); *Commonwealth Scientific and Indus. Research Org. v. Buffalo Tech., Inc.*, 542 F.3d 1363, 1370, 1378-80 (Fed. Cir. 2008) (reviewing for clear error a denial of summary judgment of invalidity, citing *Brooktree* and noting with reference to 35 U.S.C. § 132 that "[t]he question whether new matter has been added to an application is a question of fact").

For example, a "recapture" analysis requires first construing the claims. *See MBO Labs.*, 602 F.3d at 1314 (noting that the first step in applying the rule against recapture is to construe the reissued claims); *see also AIA Eng'g Ltd. v. Magotteaux Int'l S/A*, 657 F.3d 1264, 1272 (Fed.

Cir. 2011) ("The first step of the recapture test requires the application of claim construction principles to determine whether and in what aspect the reissue claims are broader than the original claims."); *In re Youman*, 679 F.3d 1335, 1347 (Fed. Cir. 2012) ("If the modified limitation does not materially narrow (or, in other cases, the limitation is eliminated), the Board must still determine whether the reissued claims were materially narrowed in other respects so that the claims have not been enlarged, and hence avoid the recapture rule.").

Finally, to whatever extent Defendant is arguing that the reissue claims are logically inconsistent with the disclosure, in the specification, of physically separate processors, any such argument is rejected for substantially the same reasons set forth above as to Defendant's argument that the reissue claims are inconsistent with the "core security teaching" of the specification. *See* Dkt. No. 66 at 6; *see also Ancora*, 744 F.3d at 739; '247 Patent at 16:22-47 ("Referring again to FIG. 9, the functions carried out by processors 920 and 940 may comprise separate, secure logical processes executing on the same physical processor") & Fig. 9.

Thus, the Court rejects Defendant's invalidity argument.

(3) Conclusion

For the reasons set forth in subsections (1) and (2), above, the Court hereby rejects Defendant's general 35 U.S.C. § 112, ¶ 2 invalidity arguments as to all asserted claims.

CONCLUSION

The Court adopts the constructions set forth in this opinion for the disputed terms of the patents-in-suit.

As further set forth above regarding the term "critical file," the Court finds that Claim 21 of the '103 Patent is invalid as indefinite.

The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.

SIGNED this 28th day of August, 2014.

Roy S. Payne

ROY S. PAYNE
UNITED STATES MAGISTRATE JUDGE

APPENDIX A

Term	Parties’ Agreement
“A computer program product comprising . . . an intelligent cellular telephone capability with a secure web browser . . . configured to:” (‘500 Patent, Claim 41)	The preamble is limiting.
“A computer program product . . . configured to . . . open the first web browser process” “A computer program product . . . configured to . . . open a first web browser process” (‘500 Patent, Claim 41; ‘528 Patent, Claim 64)	The preamble is limiting.

(Dkt. No. 52 at 1-2; Dkt. No. 68, Ex. A at 5.)